UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,157	12/21/1999	JAMES H. MOORE	D/99748	3291

7590 04/14/2004

JOHN E BECK
XEROX CORPORATION
XEROX SQUARE 20A
ROCHESTER, NY 14644

EXAMINER	
SHIN, KYUNG H	
ART UNIT	**PAPER NUMBER**
2132	4

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,157	MOORE, JAMES H.	
	Examiner	Art Unit	
	Kyung H Shin	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment received on Feb. 8, 2004.

2. Applicant amended **claim 1, 6 and 7.**

3. **Claims 1-7** are pending on this application. **Claim 1** is independent claim.

Claim Objections

4. Time Source Provider (a trusted third party) in preamble is objected to because they include reference characters, which are enclosed within parentheses or bracket. Reference characters corresponding to elements used in conjunction with the recitation of the same element or group of elements in the claims should not be enclosed within parentheses so as to avoid confusion with other numbers or characters, which may appear in the claims.

Response to Arguments

5. Applicant's arguments filed Feb. 2, 2004 have been fully considered but they are not persuasive. The applicant have argued the following:

5.1 Under remarks, applicant argued that *Haber* does not teach or suggest the steps of *generating* Private and Public Key pairs for the client and the Time Source Provider (TSP) or *using* the Key pairs for encrypting and decrypting the data and file attributes.

However, *Romney* teaches generating client key pairs (Romney, see col. 6, lines 62-63: the process begins with *client 100 generating a public-private key pair* at block 200), the data and file attributes being encrypted using the client's public/private key pair.

Doyle also discloses decrypting the encrypted data and file attributes using the server (TSP) private key and client public key combination sequence, after generation of key pairs for both client and server (TSP): (Doyle, see col. 7, lines 35-37: ...In response to the stamp request, the server (TSP) 3010 would generate a key pair for the current time interval according to an embodiment of the present invention, and see col. 7, lines 58-59: ...the client computer 3020 would generate a key pair and transmit the public key of the key pair to the server 3010....)

5.2 Under remarks, applicant argued that there is *no motivation to modify Haber* to generate a Public and Private Key pair and signature the encrypted data as taught in *Romney*.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5

USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

In this case, *Romney* teaches how *the digital signature* is made using a private key. (Romney, see col. 3, lines 9-13:, "*The sender encrypts the resulting message digest with the sender's private key. The result, the encrypted message digest, then becomes the digital signature of the electronic document. The digital signature may be appended to the electronic document or kept as a separate entity. ")*

Further, Doyle discloses generating its own public/private key pairs, whereby the two sets of key pairs are used to encrypt/decrypt or sign/verify between two entities. (Doyle, see col. 7, lines 53-66: "*In yet another alternative embodiment of the client-server architecture illustrated in FIG. 3A, ... For example, the client computer 3020 would generate a key pair and transmit the public key of the key pair to the server 3010 via connection 3030. The private key of a key pair generated by the server 3010 for the current time interval would be used to sign the public key from the client 3020. The signed public key and the public key of the key pair generated by the server would be transmitted back to the client 3020. The private key from the key pair generated by the client 3020 would be used to time stamp the data.")*

Although Haber is silent about generating key pairs, Haber utilizes Digital Signature scheme, (*Haber,* see col. 2, line 66 - col. 3, line 5: *"The TSA time-stamps the document by adding digital data signifying the current time,*

applying the agency's cryptographic signature scheme to the document, and transmitting the resulting document, now a certificate of the temporal existence of the original document, back to the author where it is held for later use in required proof of such existence."). Therefore, there is *motivation to modify Haber* to generate a Public and Private Key pair and sign the encrypted data and then verify with the other key would be a strong security practice instead of sending the digital documents in message digest value.

5.3 Under remarks, applicant argued that *Doyle* does not teach or suggest the concepts of the present application, such as generating a Public and Private Key pair for *both* the client and the Time Source Provider (TSP), and then using the Key pairs to encrypt and decrypt the files.

Doyle discloses both the client and server (TSP) generate and use key pair (Doyle, see col 7, lines 53-66: ...In yet another alternative embodiment of the client-server architecture illustrated in FIG. 3A, the client computer 3020 can generate its own key pair, and use a key pair generated by the server.....)

Therefore, the rejection of claims 1-7 is proper and maintained herein.

Claim Rejections - 35 USC § 103

6. **Claims 1-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Haber et al.* (U. S. Patent No. 5,136,647 filed on Sep. 22,1998) in view of *Romney et al.*

(U. S. Patent No. 6,085,322 filed on Sep. 22,1998) and further in view of *Doyle* (U. S. Patent No. 6, 381,696 filed on Sep. 22,1998).

Regarding claim 1, (Currently amended)

A method for securing the integrity of files prior to archiving of said files, involving an exchange between a client and a Time Source Provider (a trusted third party) said method comprising the steps of:

Haber discloses secure time-stamping of digital documents between agency and client, but Haber does not disclose specifically encrypt/decrypt with the generated key pairs. However, *Doyle* discloses,

the Time Source Provider (as server in *Doyle*) generating a public and private key pair for use in transactions with the client; (*Doyle,* see Fig. 3A, col. 7, lines 35-41: "In response to the stamp request, the server 3010 would generate a key pair for the current time interval --- (e.g., with a public key signed by the private key of the prior time interval key pair) and return the key pair ---- to the client computer 3020.")

the Time Source Provider (as recipient in *Doyle*) decrypting said encrypted data and file attributes with the Time Source Provider's Private Key and then with the client's Public Key; (*Doyle,* see col. 2, lines 51-62: "The message digest is then encrypted using the sender's secret key before sending the data to the recipient. The recipient can then use the sender's public key to automatically decrypt the message digest and then verify that it does indeed match the original data.)

Haber discloses a method of time stamping digital document (see Fig1 and col. 2, line33) and verify by signatures (see col. 2, line 44) to accept integrity of document on a reliable system prior to its transmittal to the author. Haber discloses:

a) The client (author) converts the digital document to a reduced digital size (see col. 3, line 9-11) using one-way hash (see col. 3, line 13) to meet the step of transmitting encrypted data;
b) TSP (Time Source Provider) creating a TimeMap as Time stamp receipt (see Fig. 2, step 25) containing a current time (see col. 4, line 10-12), an ID of author, a hash of document, and receipt of the data, etc for each document (see col. 4, line 8) with a variety of parameters as a string (see col. 6, line 24), and cryptographic signatures (see col. 6, line 28-30);
c) TSP returns client's data along with the certified (e.g., signature) TimeMap (see col. 4, line 23) and encryption key signatures (see col. 7, line 2);
d) TSP providing encrypted data (see step 27 and col. 6, line 57) back to the client (author) (see col. 6, line 68);

However, Haber does not disclose the client generating a key pair; generating "attributes" including "cryptographic signatures"; encrypting the file with client's public key. Haber does not disclose the client archives the original files, file attributes and time map from TSA. However, Romney discloses:

a) the client generating a Public and a Private Key pair (see Fig. 2, 200 and col. 6, line 62, 63);

b) the client generate cryptographic signature (col. 7, line 51, 52) and attached to the document (col. 7, line 60);

c) encrypting the client's files, message digest, with the private key (see col. 8, line 42);

Doyle discloses:

a) returning the client data (see col. 7, line 38) along with the session key signatures (see col. 8, line 56).

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate a Public and a Private key pair (see col. 6, line 62, 63) and sign the encrypted data as taught in Romney. Further in view to modify Haber by providing signature for the time stamped file attest to the veracity of both the content of the original data, as well as the timestamp at which the session key signature was made as taught in Doyle.

One would have been motivated to modify Haber to create a key pair and signature by client as taught in Romney in order to prevent altering the document during transmission (see col. 2, line 62, 63) from the sender to the recipient. Further, one would have been motivated to modify Haber to sign the TimeMap with the session key signature based on time differences as taught in Doyle in order to authenticate digital signature time stamps with a pair of signature keys, because signing time stamped file with a session key signature prevents tampering, which provides non-repudiation to the client authenticity (see col. 4, line 10).

Regarding claim 2, (Original) Romney discloses the client's Public/Private Key pair (see Fig. 3A, step 2010 and col. 5, line 34) is organizationally associated.

Regarding claim 3, (Original) Doyle discloses the client provides multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures (see col. 8, line 56 and 65)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Haber's time-stamp signature process to incorporate a multiple encryption of files in generating the signatures (see col. 9, line 24-28) of the encrypted files with the prepared key pairs as taught in Doyle. One would have been motivated to generate encrypt signature keys for preserving the security in order to provide rigorous proof of the time of existence and the authenticity of the content of documentation (see col. 8, line 56-58).

Regarding claim 4, (Original) Haber discloses including a sequential receipt number in generating the signatures of the encrypted files (see col. 4, line 9). However, Haber does not teach a session key in generating the signature of the encrypted files between the client and Time Source Provider for securing the transaction. However, Doyle teaches a session key (see col. 9, line 19, 20) usage in generating the signatures of the encryption of files and for securing the transaction.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Haber's time-stamp signature procedure to incorporate a secret key as the session key (see col. 2, line 39) in generating the signature of the encrypted files

as taught in Doyle. One would have been motivated to generate a random session key and encrypt it using a public key in order to secure document traffic and destroyed when it is no longer needed which reduces the risk of compromising the key.

Regarding claim 5, (Original) is rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al. U.S. Patent No. 5,136,647 in view of Doyle U.S. Patent No. 6,381,696 and further in view of Labozzeta U.S. Patent No. 5,107,269.

Haber discloses sequential numbers as a modification of the file attributes. Doyle discloses for application of the representation of the time and session key signatures (see col. 8, line 56). But, neither of them teach the application of multiple nor differing error-correcting codes. However, Labozzeta discloses multiple or differing error correcting codes (see col. 4, line 8) with source calibration data (see col. 5, line 48) to generate variable value.

It would have been obvious to one of ordinary skill in the art at the time the invention to modify Haber's time-stamp signature procedure to add the key transmitting with some kind of error detection and correction bits by adapting the error correction (see col. 4, line 18) codes taught in Labozzeta. One would have been motivated to apply representation of time and error correction codes for correcting differential in the detected value in order to prevent a garbled key in transmission to produce a precise measure of the key values and the integrity of documentation with an electronic time stamp.

Regarding claim 6, (New) Haber discloses secure time-stamping of digital documents between agency and client, but Haber does not disclose specifically the client producing said archived files, file attributes and time map; TSP retrieving time map and session key; regenerating time map; encrypting said time map with said session key and compare them. Haber also fails to disclose the client encrypting clear channel transaction using the client's key pair, and then sending clear channel transaction to the TSP. However, *Romney* discloses a method as in claim 4, further comprising the steps of:

a) the client producing said archived files, file attributes and time map; (*Romney,* see col. 7, lines 1-6)

b) the Time Source Provider retrieving said time map and session key; (*Romney,* see col. 7, lines 34-37)

c) the Time Source Provider regenerating said time map; (*Romney,* see col. 8, line 63- col. 9, line 3)

d) the Time Source Provider encrypting said time map with said session key; (*Romney,* see col. 11, line 26-28)

e) comparing said regenerated time map to said time map. (*Romney,* see col. 5, lines 19-25)

It would have been obvious to one of ordinary skill in the art, at the time of the invention was made to combine the inventions of Haber to establish the authenticity of an electronic document as taught in *Romney*. Therefore, one would be motivated to

add the stated concepts and embodiments in order to enhance the effectiveness of the authenticity of a digital signature.

Regarding claim 7,(New) A method as in claim 1, further comprising the steps of:

a) *Doyle* discloses establishing a clear channel transaction interval and pattern; (*Doyle,* see col. 7, lines 42-45: "secure SSL transactions")

d) *Doyle* discloses triggering an alarm if said clear channel transaction is not received by the Time Source Provider. (*Doyle,* see col. 7, lines 42-45: "secure SSL transactions (alarm: indication of error during transmission)")

b) *Romney* discloses the client encrypting said clear channel transaction using the client's Public and Private key pair; (*Romney,* see col. 2, lines 4-50: "public/private key processing")

c) *Romney* discloses sending said clear channel transaction to the Time Source Provider; (*Romney,* see col. 7, lines 34-37: " transmit encrypted sequence")

It would have been obvious to one of ordinary skill in the art, at the time of the invention was made to modify the inventions of Haber to establishing a clear channel transaction interval as taught in *Doyle,* and encrypting clear channel transaction using the client's key pair as taught in *Romney.* Therefore, one of ordinary skill in the art would have been motivated to combine the stated concepts and embodiments in order to secure data transmission integrity.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305-0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS

Kyung H Shin
Patent Examiner
Art Unit 2132

KHS
April 5, 2004

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100